ABSTRACT OF THE DISCLOSURE

A shared key generation apparatus is formed by integrating a random number generator for generating a random number ka that holds a relationship $0 < ka < q$ where an element in a finite group F for which multiplication is defined is g and an order as a prime number of the element g is q; a public key generator for calculating a public key ya in the finite group F using the random number ka, the element g, and the prime number q; and a shared key generator for generating a shared key Ka on the basis of a public key yb generated by a user 2 (public key distribution source and public key distribution destination) and the secret key ka generated by the random number generator, on one LSI, thereby preventing main arithmetic of the shared key generation apparatus from being revealed.